Department of Homeland Security Daily Open Source Infrastructure Report for 17 July 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports oil surged to record highs above $78 on Friday, July 14, on fears that conflict between Israel and Hezbollah guerrillas could escalate and spread to more Middle East countries. (See item 1)
- The Boston Globe reports federal highway officials have sent out a nationwide appeal seeking to identify other tunnels that rely on the same bolt−and−epoxy ceiling fasteners whose failure is now being eyed as the cause of the Big Dig tunnel tragedy. (See item 13)
- Security officials, long worried that a powerful bomb detonated in one of New York's underwater tunnels could send a torrent of water cascading through the city's labyrinth of subterranean tubes, have been spending millions to "harden" key tunnels to protect them in case of a bomb attack. (See item 16)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 14, Reuters* — **Oil soars to record $78 on Mideast conflict.** Oil surged to record highs above $78 on Friday, July 14, on fears that conflict between Israel and Hezbollah guerrillas could escalate and spread to more Middle East countries. Iran's nuclear standoff with the West,

fears over oil supply in Nigeria due to militant attacks, an influx of fund buying and falling U.S. crude supplies also buoyed the price of oil, which is up nearly 30 percent this year. U.S. crude soared to as high as $78.40 a barrel in intraday trading. Illustrating the market's sustained strength, prices for oil futures contracts to be delivered further ahead were trading above $80, from December 2006 to August 2007. "There is nothing to stop prices at the moment with the stream of headlines that are coming in. All we need now is a big hurricane," said Mike Barry of London's Energy Market Consultants.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/14/AR2006071400156.html

2. *July 13, Associated Press* — **Turkey inaugurates Caspian oil pipeline.** The presidents of Turkey, Azerbaijan, and Georgia formally opened a pipeline Thursday, July 13, designed to bypass Russia and bring Caspian oil to Europe, a route that President Bush said would bolster global energy security. The U.S. staunchly supported the 1,100−mile, $3.9 billion pipeline as part of a strategy to tap sources of crude outside of the Middle East and draw the Caspian states away from Russia and closer to the West. Oil began flowing from the Turkish port of Ceyhan last month and some 430,000 barrels of oil are flowing each day, said Norman Rodda, construction manager for the Turkish section of the pipeline. Officials at BP, the pipeline consortium's main participant and the largest foreign investor in Azerbaijan's oil sector, said they expected pumping to increase to 1 million barrels per day by 2008. The new oil is not expected to have a major impact on already sky−high oil prices, but some experts said the crude may have helped prices from going even higher. There is already talk of building new Caspian pipelines to increase the flow.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/n/a/2006/07/13/international/i074036D12.DTL&feed=rss.business

3. *July 13, Reuters* — **Record California power demand possible soon.** California's power grid could post a new electricity demand record by Monday, July 17, as air conditioners across the state battle a powerful heat wave, the California Independent System Operator said. The grid operator called on Californians to conserve electricity by calling a "power watch" from Friday to Monday, said Stephanie McCorkle, spokesperson for the ISO. The highest demand is expected Monday when the hottest temperatures are forecast in the current heat wave over most of the western United States. Monday's peak is expected to be 46,500 megawatts, also around 4 p.m. PDT. The Cal ISO called on generating plants contributing to the state's power grid to restrict plant maintenance from noon until 10 p.m. PDT on Thursday, July 13.
Source: http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006−07−13T210005Z_01_N13280710_RTRUKOC_0_US−UTILITIES−CALIFORNIA−RECORD.xml&archived=False

4. *July 13, National Nuclear Security Administration* — **U.S. nuclear weapons−grade material converted into electricity.** The Department of Energy's (DOE) National Nuclear Security Administration (NNSA), USEC Inc. and BWX Technologies, Inc. announced that enough material for 800 nuclear weapons has been converted into commercial nuclear reactor fuel. This conversation produced enough fuel to power a typical commercial nuclear reactor for approximately 34 years, generating enough electricity for power every U.S. household for 81 days or meeting 22 percent of U.S. annual household electricity needs. Approximately 50 metric tons of highly enriched uranium (HEU) was converted into nearly 660 metric tons of

low−enriched uranium (LEU) fuel. Known as the U.S. HEU Downblending Program, the conversion process began in 1999 with HEU shipments from DOE's Portsmouth Gaseous Diffusion Plant and NNSA's Y−12 National Security Complex, where the material was securely stored. "This is a major accomplishment. We have successfully turned weapons material into something people can use to turn the lights on in their house. Reducing stockpiles of surplus weapons−usable material in the U.S. and around the world is critical to global security and a key part of NNSA's mission," said NNSA Administrator Linton F. Brooks.
Source: http://www.nnsa.doe.gov/docs/newsreleases/2006/PR_2006−07−13_NA−06−25.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *July 14, News Channel 5 (TN)* — **Toxic tanker accident shuts down Interstate for hours.** Traffic was backed up for miles and residents evacuated from their homes when a tanker carrying a toxic chemical caught on fire Thursday night, July 13. The Interstate 65 was closed for a 16−mile stretch, starting just four miles north of the Tennessee line.
Source: http://www.newschannel5.com/content/news/20701.asp

[Return to top]

Defense Industrial Base Sector

6. *July 14, Aviation Week* — **Army applying lean business practices.** The U.S. Army has begun training a group of senior leaders in lean/six sigma business practices and plans to begin applying these principles across its various processes to improve efficiency, according to Army Secretary Francis Harvey. Lean/six sigma business practices seek to remove all waste from a process while ensuring quality. Once trained, these leaders will apply lean/six sigma principles across the Army, with the goal of improving the service's reset, repair, manufacturing and administrative processes. The strategy includes a greater emphasis on information technology and taking the "work out" of the system, where appropriate, Harvey said.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/LEAN07146.xml

7. *July 14, Washington Technology* — **Defense Security Service re−opens clearance business.** The Department of Defense earlier last week resumed taking applications from contractors for all types of personnel security−clearance investigations, after it had suspended processing for almost two and a half months. The Defense Security Service’s (DSS) announcement, issued Monday, July 10, said that the Defense Industrial Security Clearance Office began accepting applications for all initial investigations at the top secret, secret and confidential levels. DSS instructed industry to submit its most urgent security−clearance applications first during the next few weeks to prevent an unmanageable glut of requests.
Source: http://www.washingtontechnology.com/news/1_1/defense/28937−1 .html

8. *July 14, Government Accountability Office* — **GAO−06−839: Weapons Acquisition: DoD Should Strengthen Policies for Assessing Technical Data Needs to Support Weapon**

Systems (Report). A critical element in the life cycle of a weapon system is the availability of the item's technical data—recorded information used to define a design and to produce, support, maintain, or operate the item. Because a weapon system may remain in the defense inventory for decades following initial acquisition, technical data decisions made during acquisition can have far−reaching implications over its life cycle. In August 2004, the Government Accountability Office (GAO) recommended that the Department of Defense (DoD) consider requiring program offices to develop acquisition strategies that provide for future delivery of technical data should the need arise to select an alternative source for logistics support or to offer the work out for competition. For this review, GAO (1) evaluated how sustainment plans for Army and Air Force weapon systems had been affected by technical data rights and (2) examined requirements for obtaining technical data rights under current DoD acquisition policies. To ensure that DoD can support sustainment plans for weapon systems throughout their life cycle, including revisions to these plans aimed at achieving cost savings and complying with legislative requirements, GAO recommends improvements in DoD's acquisition policies regarding the acquisition of technical data. DoD concurred with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06839high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−839

9. *July 13, U.S. Air Force* — **Air Force, Army plan similar network modernization.** Air Force and Army officials say their plans for network modernization are similar to one another. Across the Department of Defense (DoD), the services are working to synchronize their respective operational and support networks. Eventually, the services' individual networks −− the Army with "LandWarNet," the Air Force with "ConstellationNet," and the Navy with "FORCENet" −− will all be tied together as part of DoD's Global Information Grid, or GIG, expansion project. The implementation of the GIG, the "transport," will bring a whole new spate of problems involving data synchronization. Particularly, in order to realize the synergy of having every system connected to every other system, the resources on those systems will have to speak a standard language and be able to share data seamlessly. Solving the data synchronization problem is something experts in the Army, Navy and Air Force will have to work on in order to fully leverage the GIG's overall potential.
Source: http://www.af.mil/news/story.asp?id=123023305

[Return to top]

Banking and Finance Sector

10. *July 17, El Paso Times (TX)* — **Latest phishing attempt offers IRS refunds.** The Internal Revenue Service is warning computer users about bogus e−mails claiming to be from the federal tax agency and asking for personal financial information. In a phishing scheme, computer users receive e−mails from a source that uses the IRS logo. The e−mails direct them to a Website that requests detailed personal and financial information. "We've seen an upswing in this activity lately," said Lea Crusberg, a spokesperson for the IRS in Houston. Since November, the IRS has identified 99 different scams, of which 20 came in June. More than 7,000 allegedly fake e−mails have been forwarded to the IRS, including about 1,300 in June. The number of phishing attempts is increasing. Reports tracked by the Anti−Phishing Working Group identified 11,976 phishing Websites in May of 2006, up from 3,326 in May of last year.

Source: http://www.elpasotimes.com/business/ci_4049335

11. *July 14, Websense Security Labs* — **Phishing Alert: Montgomery County Employees FCU.** Websense Security Labs has received reports of a new phishing attack that targets customers of Montgomery County Employees FCU. Users receive a spoofed e−mail message, which claims that their account will be terminated if it is not renewed. Users are directed to verify their identities by logging on. The message provides a link to a phishing Website that asks for account information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =554

12. *July 13, Associated Press* — **Treasury kills money−laundering database.** The U.S. Treasury Department pulled the plug Thursday, July 13, on a program it had heralded as an expansive new tool that would help law enforcement, counterterrorism, and intelligence officials track terrorist financing and money laundering. The program was supposed to launch later this year. The Treasury's Financial Crimes Enforcement Network (FINCEN) began developing the program in 2003, and it was meant to update older money−laundering computer−search programs. The canceled program was called BSA Direct Retrieval and Sharing because it held information obtained through the Bank Secrecy Act. FINCEN said the program's development had "repeatedly missed program milestones and performance objectives."
Source: http://www.chron.com/disp/story.mpl/ap/fn/4045244.html

[Return to top]

Transportation and Border Security Sector

13. *July 15, Boston Globe* — **Nationwide search begun for other flawed tunnels.** Federal highway officials have sent out a nationwide appeal seeking to identify other tunnels that rely on the same bolt−and−epoxy ceiling fasteners whose failure is now being eyed as the cause of the Big Dig tunnel tragedy. In an e−mail sent Thursday, July 13, to state government officials, engineers, and other tunnel specialists, a Federal Highway Administration official wrote: ``I want to know if any of your tunnels have epoxy anchor bolts as part of the support system for your suspended ceiling, jet fans, sign supports, or other equipment." Federal officials would not say how they intend to use the information, nor would they discuss any responses they had received. The collapse of massive concrete ceiling panels onto a car in the Interstate 90 connector on Monday night, July 10, has reverberated across the nation, with state officials scrutinizing their own tunnels for problems with the bolt−and−epoxy system. “We are all redoubling our efforts to make sure our ceiling systems are sound,” said Doug MacDonald, secretary of transportation for Washington State, where a tunnel uses the system.
Source: http://www.boston.com/news/traffic/bigdig/articles/2006/07/15/nationwide_search_begun_for_other_flawed_tunnels/

14. *July 15, Associated Press* — **Foreign companies buying U.S. roads, bridges.** Roads and bridges built by U.S. taxpayers are starting to be sold off, and so far foreign−owned companies are doing the buying. On a single day in June, an Australian−Spanish partnership paid $3.8 billion to lease the Indiana Toll Road. An Australian company bought a 99−year lease on Virginia's Pocahontas Parkway, and Texas officials decided to let a Spanish−American

partnership build and run a toll road from Austin to Seguin for 50 years. Few people know that the tolls from the U.S. side of the tunnel between Detroit and Windsor, Canada, go to a subsidiary of an Australian company −− which also owns a bridge in Alabama. Some experts welcome the trend. Robert Poole, transportation director for the conservative think tank Reason Foundation, said private investors can raise more money than politicians to build new roads because these kind of owners are willing to raise tolls. But to encourage more domestic investment in highways, former Department of Transportation Secretary Norman Y. Mineta made a pitch to Wall Street on May 23. "The time is now for United States investors −− including our financial, construction and engineering institutions −− to get involved in transportation investments," said Mineta, who left office July 7.
Source: http://www.usatoday.com/news/nation/2006−07−15−u.s.−highways_x.htm

15. *July 14, Boston Globe* — **Many more Big Dig flaws detected; Romney to take over probe.** More than 240 loose ceiling bolt fixtures are scattered throughout the Interstate 90 connector tunnel, said Massachusetts Turnpike Authority officials, who announced that the tunnel could remain closed for weeks as engineers determine whether to repair or replace the tunnel's drop ceiling. The suspect bolts were holding up bulky concrete ceiling panels over every lane of the heavily traveled tunnel, where panels collapsed Monday night, July 10, killing Milena Del Valle. Law enforcement officials investigating death are focused on the failure of bolt−and−epoxy fixtures. Despite the existing federal and state investigations, lawmakers on Boston's Beacon Hill and Capitol Hill −− facing unprecedented public outcry over the Big Dig's most recent and tragic failure −− called for additional probes. Massachusetts Governor Mitt Romney demanded and received legislative approval on Thursday, July 13, for his administration to take over safety inspections of the connector tunnel and to decide when and if it can reopen to traffic. The National Transportation Safety Board quickly dispatched a six−member civil engineering group to Boston to inspect the accident scene and determine whether a full−scale investigation is warranted.
Source: http://www.boston.com/news/traffic/bigdig/articles/2006/07/14/many_more_flaws_detected_romney_to_take_over_probe/

16. *July 14, Associated Press* — **Officials "harden" New York−area tunnels.** For years, security officials have worried that a powerful bomb detonated in one of New York's underwater tunnels could send a torrent of water cascading through the city's labyrinth of subterranean tubes, flooding the subways and drowning commuters. Experts are skeptical that a bomb small enough to be hidden in a bag or backpack could cause a breach in river tunnels drilled through bedrock, as many of the city's subterranean tubes are. Train operators, however, have been spending millions to "harden" key tunnels to protect them in case of a bomb attack. "It's obviously a very serious concern of ours," said Lewis Schiliro, a former FBI agent who is now director of interagency preparedness for the Metropolitan Transportation Authority, which runs the subway system. Amtrak, which has tunnels across both the Hudson and East rivers, is part way through a $472 million project to make the tubes less likely to turn into death traps during an attack or major accident. The improvements, begun in 2002, include powerful fans that can ventilate smoke, more water sources in the tunnels for firefighters and updates to the floodgates designed to seal off the tunnels in the event of a breach.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/13/AR2006071301653.html?sub=AR

17. *July 14, Department of Homeland Security* — **DHS announces major investment in next−generation radiological detection equipment.** The Department of Homeland Security (DHS) announced on Friday, July 14, the award of Advanced Spectroscopic Portal (ASP) program contracts totaling $1.157 billion to enhance the detection of radiological and nuclear materials at the nation's points of entry. DHS Secretary Michael Chertoff said, "This advanced equipment will greatly enhance our ability to manage risk and focus on the greatest threats, particularly those presented by nuclear and radiological elements." The ASP program improves upon the existing polyvinyl toluene based radiation portal monitors that are currently being deployed to the nation's points of entry by Customs and Border Protection, as well as overseas through the Department of Energy Megaports Initiative. These new systems will enhance current detection capabilities by more clearly identifying the source of detected radiation through spectroscopic isotope identification. The priority for the first year is development and testing of the fixed radiation detection portal that will become the standard installation for screening cargo containers and truck traffic.
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0952.xml

18. *July 14, Washington Post* — **Bribery at border worries officials.** Federal law enforcement officials are investigating a series of bribery and smuggling cases in what they fear is a sign of increased corruption among officers who patrol the Mexican border. Two brothers who worked for the U.S. Border Patrol disappeared in June while under investigation for smuggling drugs and immigrants, and are believed to have fled to Mexico. In the past month, two agents from Customs and Border Protection, which guards border checkpoints, were indicted for taking bribes to allow illegal immigrants to enter the United States. And earlier this month, two Border Patrol supervisory agents pleaded guilty to accepting nearly $200,000 in payoffs to release smugglers and illegal immigrants who had been detained. Authorities say two factors are causing concern that larger problems may develop: The massive buildup of Border Patrol agents in recent years has led to worries that hiring standards have been lowered; and, as smugglers demand higher and higher fees to bring illegal immigrants into the United States, their efforts to bribe those guarding the border have intensified. While the main corruption problem along the border is still among Mexican law enforcement officials, there have been numerous arrests of U.S. officers, too.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07 /14/AR2006071401525.html?sub=AR

19. *July 14, Associated Press* — **Low−cost carriers seek bigger stake of airline traffic.** Low−cost carriers are extending their push into the territory of their bigger competitors, with JetBlue Airlines Corp. announcing Thursday, July 13, that it will expand to Ohio and Southwest Airlines Co. ready to debut in Washington, DC. The New York−based JetBlue said it will begin providing daily non−stop flights in October between Port Columbus International Airport and New York and Boston, offering introductory one−way fares as low as $69. Dallas−based Southwest on Thursday announced one−way fares as low as $79 for new daily non−stop flights between Washington Dulles International Airport and four cities. The carriers are leading the way toward a low−cost model in an industry in which several major airlines have filed for bankruptcy in recent years, said Frank Werner, a finance professor at Fordham University in New York. Defining low−cost airlines has become more difficult because there are times when the traditional carriers have lower prices for some flights than the low−cost airlines, said John Heimlich, chief economist at the Air Transport Association trade organization.

Source: http://www.usatoday.com/travel/flights/2006−07−14−lowcost−st rategies_x.htm

[Return to top]

Postal and Shipping Sector

20. *July 14, New York Times* — **Powder sent to New York Times not anthrax.** Police and environmental workers responded to the New York Times offices on Friday, July 14, after an employee in the postal services department opened a letter addressed to the newspaper and saw a powdery substance he believed to be suspicious, the police said. The letter had a postmark from Philadelphia, the police said, and contained an editorial published by The New York Times on June 28 titled “Patriotism and the Press,” with a red “X” written across it, said Paul J. Browne, the Police Department’s chief spokesperson. The employee, a 54−year−old man from Brooklyn, followed procedures established by the newspaper after opening the envelope. He immediately placed the letter in a plastic bag and alerted his supervisor, who dialed 911, the police said. Once the substance was deemed non−threatening, Browne said the entire episode appeared to be a hoax, noting the juxtaposition of a defaced editorial in an envelope with cornstarch.
Source: http://www.nytimes.com/2006/07/14/nyregion/14cnd=powder.html ?ex=1153108800&en=dfb44543b16a398a&ei=5087

[Return to top]

Agriculture Sector

21. *July 14, Agence France−Presse* — **Romanian swine fever worrying.** European Health Commissioner Markos Kyprianou has expressed concern at an epidemic of swine fever which has affected central and northern Romania for the past two years. He told a press conference the European Union would be sending teams of experts to study the situation before September. Romanian Agriculture Minister Gheorghe Flutur said the number of outbreaks of the disease had been reduced from 1,500 last year to 65, and it was hoped to eradicate it by the end of the year. But he warned that it could break out again at any time, with small breeders raising more than four million pigs in the country.
Swine fever information: http://www.oie.int/eng/maladies/fiches/a_A130.htm
Source: http://news.yahoo.com/s/afp/20060714/hl_afp/romaniahealthfar meu_060714145400;_ylt=Arm4H3EwxxLozSP58txU0F.JOrgF;_ylu=X3oD MTA5aHJvMDdwBHNlYwN5bmNhdA−−

22. *July 13, Reuters* — **U.S. to join Canadian mad cow investigation.** The Canadian Food Inspection Agency confirmed on Thursday, July 13, that an Alberta dairy cow had tested positive for mad cow disease, an announcement that raised enough concern in Washington for it to send an expert to join the investigation. "We need a thorough understanding of all the circumstances involved in this case to assure our consumers that Canada's regulatory system is effectively providing the utmost protections to consumers and livestock," U.S. Agriculture Secretary Mike Johanns said. "I am dispatching a USDA (U.S. Department of Agriculture) expert to participate in the investigation of this case, particularly as it relates to how this animal

may have been exposed to infected material," Johanns said. The 50−month−old cow, which died on the Alberta dairy farm where it was born, is Canada's seventh mad cow case since 2003.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/13/AR2006071301379.html

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

23. *July 12, North County Times (CA)* — **Warner schools forced to turn off drinking fountains.** San Diego, CA, health officials ordered Warner Springs schools to shut down all the drinking fountains on campus this week after discovering that bacteria has contaminated the water supply, the county announced Wednesday, July 12. Routine test results −− confirmed by retesting done Tuesday, July 11 −− revealed that coliform bacteria was present in the water that supplies the district's campus, which is home to both an elementary school and a middle/high school. The county issued an order requiring that the district's well water be boiled before anyone is allowed to drink it, said Mark McPherson, the chief of land and water quality for the county's Department of Environmental Health.
Source: http://www.nctimes.com/articles/2006/07/13/news/sandiego/21_41_357_12_06.txt

[Return to top]

Public Health Sector

24. *July 16, Reuters* — **India claims poultry bird flu vaccine.** India announced on Sunday, July 16, it has successfully developed a vaccine against bird flu in poultry. The country has culled hundreds of thousands of birds since February when it reported its first outbreak in poultry. Although no human infections have been reported, thousands of people were monitored for flu−like symptoms. "I am happy to announce the high security animal disease laboratory (in) Bhopal ... has made significant effort to develop a killed vaccine against the bird flu in a short period of time," Agriculture Minister Sharad Pawar said in New Delhi. The laboratory in Bhopal is the main facility in the country for testing and research. India is not developing a vaccine for humans but has imported vaccines for poultry from the Netherlands.
Source: http://in.today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006−07−16T122319Z_01_NOOTR_RTRJONC_0_India−25973 8−1.xml

25. *July 16, Associated Press* — **Indonesian man dies from bird flu.** A 44−year−old man died of bird flu in Indonesia, a senior health official said Sunday, July 16, putting the country on the cusp of being the world's hardest hit by the disease. If the diagnosis by a local lab is confirmed by a World Health Organization−sanctioned test, the number of people killed by bird flu in

Indonesia would rise to at least 42, tying it with hardest−hit Vietnam. The man died July 12 after being hospitalized for two days with high fever, coughing and breathing difficulties, said the official, Nyoman Kandun. The man was from eastern outskirts of the capital Jakarta and had reportedly had contact with birds.
Source: http://abcnews.go.com/Health/wireStory?id=2197214

26. *July 16, Agence France−Presse* — **Malaysian state battles fresh round of hand, foot and mouth disease.** The eastern Malaysian state of Sarawak is battling a fresh outbreak of hand, foot and mouth disease, with authorities urging parents to cancel children's social events to curb the virus. Sarawak's Deputy Chief Minister George Chan said 44 new cases had been detected on Sunday, July 16, with 10 children hospitalized throughout the state. The state on Saturday, July 15, recorded 56 new cases of the disease, which mainly affects infants and young children. The virus has affected over 12,000 children in Sarawak since an initial outbreak at the end of January and the second round, which started in early May. Eleven children have died from the disease so far.
Hand, foot, and mouth disease information: http://edcp.org/factsheets/handfoot.html
Source: http://news.yahoo.com/s/afp/20060716/hl_afp/malaysiahealthdisease_060716143357;_ylt=AvX0_t9u5p41pKp_tpJZsYaJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

27. *July 15, Department of Homeland Security* — **Statement of support by Secretary Chertoff on the Global Initiative to Combat Nuclear Terrorism.** On July 15, Department of Homeland Security Secretary Chertoff made the following announcement, “The proliferation of weapons of mass destruction and the reality of nuclear terrorism pose a deadly threat to the United States and the world. To strengthen our collective capacity to prevent and protect against this threat, President Bush and President Putin have launched the Global Initiative to Combat Nuclear Terrorism. Our nations are expanding the global fight against nuclear terrorism by enhancing the international community’s ability to detect nuclear materials and radiological substances. The Global Initiative will also assist in preventing the illicit trafficking of these materials, as well as potential hostile actions against nuclear facilities. The Department of Homeland Security is responsible for assessing the vulnerabilities of the nation’s security threats and takes the lead in coordinating with other federal, state, local, and private entities to ensure the most effective response. In furtherance of those responsibilities, we are adopting this Global Initiative, which adds to our current layered approach of deterrence and response while improving our capabilities as well as those of our international partners to search for, seize, and establish safe control over unlawfully held material.”
Source: http://www.dhs.gov/dhspublic/display?content=5742

[Return to top]

Emergency Services Sector

28. *July 14, Northender (NY)* — **In New York, Suffolk's north shore gets expanded police radio coverage.** Suffolk County, NY, Executive Steve Levy signed two bills that authorize funds to install 800 MHZ emergency services radio towers at three north shore locations which had experienced gaps in service – Rocky Point, Northport and Lloyd Harbor. "We have been working with our police department and the varying levels of government to address the problems of emergency services communications along the hilly areas of the north shore," said Levy. "With these two resolutions we can begin to finalize our agreements for the placement of these necessary towers."
Source: http://www.northender.com/northend_news_details.jsp?id=369

29. *July 13, Examiner (MD)* — **Five−stage drill tests abilities of first responders in Harford County, Maryland.** A school bus explosion, students shot, a boat crash, and hostage situations −− all in a day's work for Harford County, MD, emergency responders. At least they were on Wednesday, July 12, when a five−stage drill, meant to test the capabilities of emergency responders, kicked off in Havre de Grace with the bus explosion around 11:30 a.m. "We have learned a lot. We have learned what we need to improve upon, and what we have done well," said Havre de Grace Police Chief Teresa Walter. She said, in general, communications needed improvement, but she was surprised at how well all of the agencies involved worked together.
Source: http://www.examiner.com/a−174816~Five_stage_drill_tests_abilities_of_Harford_s_first_responders.html

30. *July 13, North Country Gazette (NY)* — **Disaster training center opens ahead of schedule.** The new state−of−the−art New York State Preparedness Training Center which serves as the hub for emergency response training for natural, technological and terrorism related disasters for first responders at all levels of government has opened in Oneida County ahead of schedule and has begun conducting training classes this week. Governor George E. Pataki first unveiled plans for the center in his State of the State Address in January 2005. The Governor announced the selection of the Oneida County Airport as the site of the center last December and provided $4.5 million for its development and staffing. Also planned at the site is the construction of a state−of−the−art emergency operations center for Oneida County and New York State agencies. The operations center, also known as a command center, will provide a practical classroom setting for first responders across the state. Additionally, it could be utilized by Oneida, neighboring counties and state agencies in the event a catastrophic event or disaster occurs in the central part of the state.
Source: http://www.northcountrygazette.org/articles/071306TrainingCe nter.html

[Return to top]

Information Technology and Telecommunications Sector

31. *July 14, Secunia* — **McAfee ePolicy Orchestrator directory traversal vulnerability.** A vulnerability has been reported in McAfee ePolicy Orchestrator, which can be exploited to compromise a vulnerable system. Analysis: The vulnerability is caused due to an input validation error in the management console's Framework Service component (enabled by default on all servers and agents). This can be exploited to write files to arbitrary locations on the system via directory traversal attacks in a specially crafted "PropsResponse" request sent to the service.

Vulnerable: McAfee ePolicy Orchestrator 3.x.
Solution: Update to version 3.5.5 or later:
https://secure.nai.com/us/forms/downloads/upgrades/login.asp
Source: http://secunia.com/advisories/21037/

32. *July 14, Secunia* — **F−Secure Messaging Security Gateway sendmail vulnerability.** F−Secure has acknowledged a vulnerability in F−Secure Messaging Security Gateway, which can be exploited by malicious people to cause a denial−of−service. Analysis: The vulnerability is caused due to an error in the termination of the recursive "mime8to7()" function when performing MIME conversions. This can be exploited to cause a certain sendmail process to crash when it runs out of stack space while processing a deeply nested malformed MIME message. Successful exploitation causes the delivery of other queued messages to fail or causes the generated core dump files to fill up available disk space.
Vulnerable: F−Secure Messaging Security Gateway P−Series; F−Secure Messaging Security Gateway X−Series.
Solution: Hotfixes have been distributed automatically by the delivery system.
F−Secure Advisory: http://www.f−secure.com/security/fsc−2006−5.shtml
Source: http://secunia.com/advisories/21042/

33. *July 14, Websense Security Labs* — **Malicious Website / Malicious Code: World Cup Final Trojan Horse.** Websense Security Labs has discovered a new malicious Website, which is distributing malicious code that installs a Trojan Horse on end−users' machines. This potentially occurs without user interaction. The site appears to be mirroring a World Cup 2006 Soccer Website with the exception that they have a lead story regarding the, now infamous, Zinedine Zidane head butt incident from the World Cup final against Italy. Upon visiting any of the pages on the site, end−users are potentially infected with a Trojan Horse downloader. This Trojan Horse downloads additional payload code from the site.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=553

34. *July 13, Information Week* — **State Department releases details of computer system attacks.** The State Department confirmed that attacks last month on some of its computer systems originated in the East Asia−Pacific region, targeting U.S. embassies there, and worked their way toward State's headquarters in Washington, DC. The department hasn't indicated whether it has a specific suspect (or suspects) in mind, but State says it's working with Carnegie Mellon University's Computer Emergency Response Team and the FBI on an investigation. The systems affected by the hack were unclassified computer systems, State Department spokesperson Sean McCormack said during a press briefing Wednesday, July 12. The State Department has taken some precautionary steps, including changing some passwords.
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=Q1GD0UEWD50OYQSNDLPSKHSCJUNN2JVN?articleID=190303153

35. *July 13, eWeek* — **Microsoft confirms PowerPoint zero−day attack.** For the third time in two months, a zero−day vulnerability in a widely used Microsoft Office software application is being used in targeted hacker attacks. The latest attack exploits a previously undocumented flaw in Microsoft PowerPoint, the ubiquitous presentation program used by millions of users around the world. The attack comes just days after Microsoft's July Patch Tuesday and closely mirrors the situation in June when a zero−day Excel attack was discovered 24 hours after Patch

Day.
Source: http://www.eweek.com/article2/0,1895,1988874,00.asp

36. *July 13, Search Security* — **CSI/FBI survey: Data breaches still being swept under the rug.** On the surface, the results of the 11th annual CSI/FBI Computer Crime and Security Survey are positive, with fewer companies reporting financial loss from data breaches compared to last year. But a majority of companies are still reluctant to report security breaches to law enforcement, suggesting that the survey isn't capturing the full extent of the problem. The Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad released its 2006 report Thursday, July 13, after surveying 616 computer security practitioners in U.S. corporations, government agencies, financial and medical institutions and universities. The average loss reported by respondents was $167,713, an 18 percent decrease over last year's average loss of $203,606.
CSI/FBI Survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml
Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1199280,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of multiple vulnerabilities in Microsoft Internet Explorer (IE) 6.0. US−CERT is also aware of a public blog that will be posting new web browser bugs on a daily basis in July. US−CERT will be analyzing relevant vulnerabilities, as well as actively monitoring the site to provide additional information as it becomes available. Please review URL: http://metasploit.blogspot.com/2006/07/month−of−browser−bugs .html

US−CERT strongly recommends the following:

Review VU#159220 / Microsoft Internet Explorer vulnerable to heap overflow via the HTML Help Control "Image" property : http://www.kb.cert.org/vuls/id/159220

Disable ActiveX as specified in the following:

Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Do not follow unsolicited links.

Review the steps described in Microsoft's document to improve the safety of your browser: http://www.microsoft.com/athome/security/online/browsing_saf ety.mspx

US−CERT will continue to update current activity as more information becomes available.

Public Exploit Code for Unpatched Vulnerabilities in Microsoft Internet Explorer

US−CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100: http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108): http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser: http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ: http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Top 10 Target Ports	1026 (win−rpc), 11890 (−−−), 38566 (−−−), 6999 (iatp−normalpri), 445 (microsoft−ds), 25 (smtp), 32790 (−−−), 80 (www), 135 (epmap), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *July 14, Associated Press* — **Carbon monoxide leak at college dorm leaves one dead, more than 100 sick.** Carbon monoxide leaked into a college dormitory early Friday, July 14, killing a man and sickening more than 100 teenagers and adults attending summer programs at Roanoke College, in Roanoak, VA, the school said. College spokesperson Teresa Gereaux said the victims were taken to two Roanoke Valley hospitals in ambulances or vans after complaining of headaches, nausea, dizziness and shakiness. An elderly man died before reaching the hospital, said Nancy May, a spokesperson for Lewis−Gale Medical Center. Others described the scene in the dorm Friday morning as chaotic. About 100 of the dormitory guests had traveled from across Virginia, North Carolina, and Pennsylvania to attend a three−day Lutheran church conference. Shortly before dawn, people staying there called campus police from the dorm's emergency phone, and the police notified the Salem Fire Department. The source of the carbon monoxide leak had not been located by noon, fire officials said.
Source: http://www.usatoday.com/news/nation/2006−07−14−carbonmonoxid e_x.htm

[Return to top]

General Sector

38. *July 14, Associated Press* — **Two California wildfires merge into one.** Thousands of firefighters aided by aircraft worked Friday, July 14, in fierce heat to keep two big wildfires from gaining a foothold in the heavily populated San Bernardino Mountains, where millions of trees killed by drought and bark beetles could provide explosive fuel. The lightning−caused fires, covering more than 95 square miles combined, merged Friday afternoon. Wildfires can grow more unpredictable after merging, but the two blazes were moving slowly Friday and U.S. Forest Service officials said it appeared that their combination was unlikely to seriously increase fire activity. The larger of the two fires has destroyed 45 homes and 118 outbuildings and remained a potential threat to 1,500 homes, said Kristel Johnson of the U.S. Forest Service. The 53,000−acre blaze started a week ago on the Mojave Desert floor below the eastern flank of the San Bernardino Mountains, and was 20 percent contained. The smaller fire had burned 8,300 acres, mostly at higher elevations. Meteorologists had bad news for firefighters in southern Montana and California's Mojave Desert and foothills: Both parched areas were expected to see weekend thunderstorms that could trigger more lightning−caused wildfires.
Source: http://www.cnn.com/2006/US/07/14/wildfires.ap/index.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer